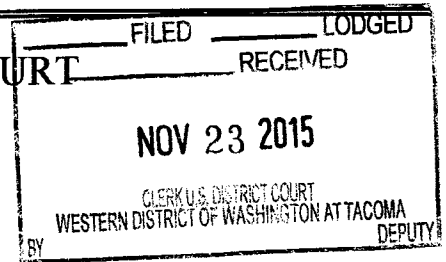


UNITED STATES DISTRICT COURT

for the
Western District of Washington



In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

5809 136th Street E, Puyallup, WA 98373 et al.

Case No.

MT 15-5212

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachments A-1, A-2, and A-3, which are incorporated herein by reference

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 875(c) and 1958(a).	Interstate threats and murder for hire

The application is based on these facts:

See Affidavit of Special Agent David J. Rubel, which is incorporated herein by reference

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent David J. Rubel

Printed name and title

Sworn to before me and signed in my presence.

Date: Nov. 23, 2015

Judge's signature

City and state: Tacoma, WA

Magistrate Judge Karen L. Stromborn

Printed name and title

1 **AFFIDAVIT**

2 STATE OF WASHINGTON)
 3) ss
 4 COUNTY OF PIERCE)

5 I, David J. Rubel, having been duly sworn, state as follows:

6 **INTRODUCTION AND AGENT BACKGROUND**

7 1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and
 8 have been so employed since 2012. I am currently assigned to the Sacramento Division
 9 of the FBI, where I investigate domestic terrorism matters, and criminal violations
 10 relating to cybercrimes, including those arising from the interstate transmission of threats
 11 via the Internet. I am a graduate of the University of Maryland, having earned a Bachelor
 12 of Science degree in Computer Science. I am also a graduate of the FBI Academy in
 13 Quantico, Virginia. I am authorized to investigate crimes involving threats of violence,
 14 including threats conveyed via the Internet, and the interstate solicitation of murder-for-
 15 hire.

16 2. I make this affidavit in support of an application under Rule 41 of the
 17 Federal Rules of Criminal Procedure for a warrant to search the premises located at 5809
 18 136th Street E, Puyallup, WA 98373 (hereinafter, the "SUBJECT PREMISES") as more
 19 fully described in Attachment A-1 to this Affidavit, a 2013 Dodge Ram truck with
 20 Washington license plate number B09802X (VIN Number 3C6JR6AG8DG515152)
 21 (hereinafter, the "SUBJECT VEHICLE") as more fully described in Attachment A-2 to
 22 this Affidavit, and SCOTT ANTHONY ORTON, as more fully described in Attachment
 23 A-3 to this Affidavit, for the property and items described in Attachment B to this
 24 Affidavit, as well as any digital devices or other electronic storage media located therein.

25 3. The facts set forth in this Affidavit are based on my own personal
 26 knowledge; knowledge obtained from other individuals during my participation in this
 27 investigation, including other law enforcement officers; review of documents and records
 28 related to this investigation; communications with others who have personal knowledge

1 of the events and circumstances described herein; and information gained through my
2 training and experience.

3 4. Because this Affidavit is submitted for the limited purpose of establishing
4 probable cause in support of the application for a search warrant, it does not set forth
5 each and every fact that I or others have learned during the course of this investigation. I
6 have set forth only the facts that I believe are necessary to establish probable cause to
7 believe that evidence, fruits and instrumentalities of violations of 18 U.S.C. § 875(c),
8 which makes it a crime to transmit in interstate or foreign commerce any communication
9 containing any threat to kidnap any person or any threat to injure the person of another;
10 and 18 U.S.C. § 1958(a), which makes it a crime to travel or cause another to travel in
11 interstate or foreign commerce, or use or cause another to use the mail or any facility of
12 interstate or foreign commerce, with intent that a murder be committed in violation of the
13 laws of any State or the United States as consideration for the receipt of, or as
14 consideration for a promise or agreement to pay, anything of pecuniary value, or conspire
15 to do so, will be found at the SUBJECT PREMISES, in the SUBJECT VEHICLE, and on
16 SCOTT ANTHONY ORTON.

17 **THE INVESTIGATION**

18 5. This is an investigation regarding threats and statements soliciting a
19 murder, which were posted on a website by SCOTT ANTHONY ORTON using the
20 online moniker "Joseywhales." The threats and solicitations, which are set forth below,
21 were directed at an officer of StemExpress, LLC, hereinafter "Victim 1." StemExpress,
22 LLC is a company that supplies human tissue for biomedical research. The company's
23 headquarters is located in Placerville, California. When the threats against, and
24 solicitation to murder, Victim 1 were conveyed, Victim 1 resided in the Eastern District
25 of California.

26 6. The statements at issue were posted on the website nation.foxnews.com
27 (hereinafter "Fox Nation"), which is a website that is administered by Fox News
28 Network, LLC (hereinafter "Fox News"). The Fox Nation website features news

1 articles, video clips, and links to editorial blogs. Visitors to the Fox Nation website can
 2 post comments on the website's comments page. Based on evidence gathered during
 3 this investigation, there is probable cause to believe that SCOTT ANTHONY ORTON
 4 posted the statements set forth below on the Fox Nation website, in violation of 18
 5 U.S.C. §§ 875(c) and 1958(a).

6 TECHNICAL TERMS

7 7. Based on my training and experience, I use the following technical terms to
 8 convey the following meanings:

- 9 a. IP Address: The Internet Protocol address (or simply "IP address") is
 10 a unique numeric address used by computers on the Internet. An IP
 11 address looks like a series of four numbers, each in the range 0-255,
 12 separated by periods (e.g., 121.56.97.178). Every digital device
 13 attached to the Internet must be assigned an IP address so that
 14 Internet traffic sent from and directed to that digital device may be
 15 directed properly from its source to its destination. Most Internet
 16 service providers control a range of IP addresses. Some computers
 17 have static—that is, long-term-IP addresses, while other computers
 18 have dynamic—that is, frequently changed-IP addresses.
- 19 b. Internet: The Internet is a global network of computers and other
 20 electronic devices that communicate with each other. Due to the
 21 structure of the Internet, connections between devices on the Internet
 22 often cross state and international borders, even when the devices
 23 communicating with each other are in the same state.
- 24 c. Domain Name: Domain names are common, easy to remember
 25 names associated with an Internet Protocol address (defined above).
 26 For example, a domain name of "www.usdoj.gov" refers to the
 27 Internet Protocol address of 149.101.1.32. Domain names are
 28 typically strings of alphanumeric characters, with each level
 delimited by a period. Each level, read backwards – from right to
 left – further identifies parts of an organization. Examples of first
 level or top-level domains are typically .com for commercial
 organizations, .gov for the United States government, .org for
 organizations, and .edu for educational organizations. Second level
 names will further identify the organization; for example usdoj.gov
 further identifies the United States governmental agency to be the
 Department of Justice. Additional levels may exist as needed until

each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

- d. Electronic Storage media: Electronic Storage media is any physical object upon which data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

8. As described above and in Attachment B, this application seeks permission to search for evidence, fruits and/or instrumentalities that might be found at the SUBJECT PREMISES, in the SUBJECT VEHICLE, and on SCOTT ANTHONY ORTON in whatever form they are found. One form in which the evidence, fruits, and/or instrumentalities might be found is data stored on digital devices¹ such as computer hard drives or other electronic storage media. Thus, the warrant applied for would authorize the seizure of digital devices or other electronic storage media or, potentially, the copying of electronically stored information from digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

9. **Probable cause.** Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents, and my training and experience, I submit that if a digital device or other electronic storage media is found at the SUBJECT PREMISES, in the SUBJECT VEHICLE, or on SCOTT ANTHONY ORTON, there is probable cause to believe that evidence, fruits, and/or

¹ "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

1 instrumentalities of the crimes of 18 U.S.C. §§ 875(c) and 1958(a) will be stored on
 2 those digital devices or other electronic storage media. I believe digital devices or other
 3 electronic storage media are being used to transmit threats of violence and solicit murder-
 4 for-hire.

5 10. On July 19, 2015, agents received tips via the FBI Public Access Line that
 6 threats were made against Victim 1. In response to the tips, I reviewed the Fox Nation
 7 website and identified threatening statements directed at Victim 1. The statements were
 8 posted by the Fox Nation user "Joseywhales."

9 11. During my review of the Fox Nation website, I learned that in order to post
 10 a statement in the website's comment section, one must first create a Fox Nation
 11 account. In order to create an account, the putative user must provide a name, physical
 12 address, and email address.

13 **Fox Nation Users Joseywhales and Joseywhales**

14 12. On August 26, 2015, Fox News provided information associated with the
 15 Fox Nation accounts for users Joseywhales and Joseywhales. In addition to the user-
 16 provided identifying information described above—i.e., the user's name, physical
 17 address, and email address— Fox News provided the IP address assigned to the
 18 electronic device that was used to create the accounts. Specifically, Fox News provided
 19 the following information:

20 **Account display Name:** "Joseywhales"

21 **User ID:** 2e5c7334-d0f8-42de-bf6a-16d50dd7cbcc

22 **Subscriber name provided by user:** Scott Orton

23 **Address provided by user:** Washington, United States, 93737

24 **E-mail address provided by user:** none

25 **Dates of service:** September 18, 2012 – September 18, 2012

26 **IP address(es):** none
 27
 28

Account display Name: "JoseywhaIes"

User ID: 6154e4b6-0c59-4beb-b4f9-0d16b789b7d6

Subscriber name provided by user: Bart Simpson

Address provided by user: WA, APO/FPO/DPO

E-mail address provided by user: scottorton@me.com

Dates of service: September 26, 2012 – present

IP address(es): 24.19.67.214; 73.181.138.175

Threats and Solicitation of Murder-For-Hire

13. On September 25, 2015, I obtained from Fox News a list of statements posted on the Fox Nation website by Fox Nation user JoseywhaIes. Along with the list of statements, Fox News provided the dates on which the statements were posted to the Fox Nation website, as well as the IP address assigned to the digital device used to post the statements. Below are JoseywhaIes's statements (and related information) concerning Victim 1:

Comment ID	Comment Created Date (GMT)	IP Address	Comment ¹
347326166	July 16, 2015; 16:21	73.181.138.175	The management of StemExpress should be taken by force and killed in the streets today.
347326390	July 16, 2015; 16:21	73.181.138.175	Kill StemExpress employees. I'll pay you for it.
347326654	July 16, 2015; 16:22	73.181.138.175	Stop the death of innocents. Kill the killers.
347327170	July 16, 2015; 16:22	73.181.138.175	StemExpress your lives don't matter nearly as much as your deaths do.
347327398	July 16, 2015; 16:23	73.181.138.175	Innocent lives matter. StemExpress employees' lives don't.

¹ The victim's name and position at StemExpress have been replaced with the terms "Victim 1" and "officer" to protect the identity of the victim.

347348862	July 16, 2015; 16:58	73.181.138.175	The [officer] of StemExpress is a death-profitier. The [officer] of StemExpress should be hung by the neck using piano wire and propped up on the lawn in front of the building with a note attached...
347349991	July 16, 2015; 17:00	73.181.138.175	[Victim 1 officer] StemExpress Inc. lives in Placerville CA. I'm going there.
347350267	July 16, 2015; 17:01	73.181.138.175	I'll pay ten grand to whomever beats me to [Victim 1]...
347350691	July 16, 2015; 17:01	73.181.138.175	[Victim 1 officer] StemExpress Inc. must die to save the innocents.
347350952	July 16, 2015; 17:02	73.181.138.175	[Victim 1] your life isn't worth squat.
347352243	July 16, 2015; 17:04	73.181.138.175	[Victim 1's] life is in more danger than Trumps. I'm here. El Chapo is in Mexico.
347352770	July 16, 2015; 17:05	73.181.138.175	[Victim 1] must die. End of story. If we as humanity accept her actions we're to be judged in the harshest manner possible.
347355967	July 16, 2015; 17:11	73.181.138.175	I'll take care of [Victim 1] myself.
347356248	July 16, 2015; 17:11	73.181.138.175	I'm going to Placerville this weekend.
347359093	July 16, 2015; 17:16	73.181.138.175	[Victim 1] will have to face the souls of the babies she's bought and sold when she arrives on the other side. I'm sending her there early.
347360148	July 16, 2015; 17:18	73.181.138.175	StemExpress employees you're on notice. You need to pay for what you've done.
347360416	July 16, 2015; 17:18	73.181.138.175	Everyone at StemExpress should be executed on live TV.
347460949	July 16, 2015; 20:08	73.181.138.175	Someone needs to double tap the [officer] of StemExpress. She lives in Placerville CA.
347467546	July 16, 2015; 20:20	73.181.138.175	I think I'll take a little trip to Placerville this weekend. I hear there's some good hunting down Placerville way...
347794919	July 17, 2015; 14:05	73.181.138.175	[Victim 1 officer] of StemExpress should be executed by hanging.

**SCOTT ANTHONY ORTON'S Email Address Is Linked
to the Joseywhales Account**

14. The email address listed on the account profile for Joseywhales—the user who posted the statements listed above—is scottorton@me.com. Apple Inc. hosts the email accounts for the me.com domain. On September 25, 2015, Apple Inc. provided subscriber records for the email account scottorton@me.com. Apple Inc. records identified the subscriber as:

Scott Orton

5809 136th St. E.

Puyallup, Washington

Day telephone number: [REDACTED]

The Threats Were Sent From SCOTT ANTHONY ORTON'S IP ADDRESS

15. In September 2015, I performed a WHOIS lookup query on a publicly available database that stores the registered users and assignees of Internet resources—such as an IP address block—to identify the Internet service provider administering the IP address 73.181.138.175 in July of 2015. From my search, I determined that Comcast Corporation administered that IP address.

16. On October 20, 2015, I obtained Comcast records identifying the subscriber for the account assigned to IP address 73.181.138.175 on July 16, 2015, at 17:01 (GMT). Fox Nation user Joseywhales posted the statement “I’ll pay ten grand to whomever beats me to [Victim 1]...” from IP address 73.181.138.175 on July 16, 2015, at 17:01 (GMT). Comcast records indicate that the foregoing IP address was assigned to SCOTT ANTHONY ORTON. Comcast provided the following additional information:

Subscriber Name: Scott Orton

Service Address: 5809 136th Street E, Puyallup, WA 98373-5117

Telephone Number: 253-537-5157

Type of Service: High Speed Internet Service

Account Number: 8498350172966724

1 **Start of Service:** Unknown

2 **Account Status:** Active

3 **IP Assignment:** Dynamically Assigned

4 **E-mail User IDs:** Scott6724

5
6 **Additional Information Linking Orton to the SUBJECT PREMISES**

7 17. On October 21, 2015, I obtained Washington State Department of
8 Licensing records regarding SCOTT ANTHONY ORTON. The Department of
9 Licensing driver's license records indicate that SCOTT ANTHONY ORTON resides at
10 5809 136th Street E, Puyallup, WA 98373. According to public records searches,
11 SCOTT ANTHONY ORTON is the only known person living at the SUBJECT
12 PREMISES. Moreover, no other individuals were spotted at the SUBJECT PREMISES
13 during recent surveillance.

14 **Information Linking Orton to the SUBJECT VEHICLE**

15 18. The Washington Department of Licensing records also indicate that at least
16 one vehicle is registered to SCOTT ANTHONY ORTON: a 2013 Dodge Ram, license
17 plate number: B09802X, VIN Number: 3C6JR6AG8DG515152 (i.e., the SUBJECT
18 VEHICLE). On November 11, 2015, agents observed the SUBJECT VEHICLE parked
19 in the open garage attached to the SUBJECT PREMISES. As a vehicle under SCOTT
20 ANTHONY ORTON's control, the SUBJECT VEHICLE is a means by which SCOTT
21 ANTHONY ORTON could travel to Placerville, California to carry out the acts
22 described in the threats and solicitations set forth above. Accordingly, there is probable
23 cause to believe that the SUBJECT VEHICLE contains evidence, fruits and/or
24 instrumentalities of the crimes of 18 U.S.C. §§ 875(c) and 1958(a).

25 19. There is, therefore, probable cause to believe that evidence, fruits and/or
26 instrumentalities of the crimes of 18 U.S.C. §§ 875(c) and 1958(a) exists and will be
27 found on digital devices or other electronic storage media at the SUBJECT PREMISES,
28

1 in the SUBJECT VEHICLE, and on SCOTT ANTHONY ORTON for at least the
2 following reasons:

- 3 a. Based on my knowledge, training, and experience, I know that computer
4 files or remnants of such files can be preserved (and consequently also then
5 recovered) for months or even years after they have been downloaded onto
6 a storage medium, deleted, or accessed or viewed via the Internet.
7 Electronic files downloaded to a digital device or other electronic storage
8 medium can be stored for years at little or no cost. Even when files have
9 been deleted, they can be recovered months or years later using forensic
10 tools. This is so because when a person "deletes" a file on a digital device
11 or other electronic storage media, the data contained in the file does not
12 actually disappear; rather, that data remains on the storage medium until it
13 is overwritten by new data.
14
- 15 b. Therefore, deleted files, or remnants of deleted files, may reside in free
16 space or slack space—that is, in space on the digital device or other
17 electronic storage medium that is not currently being used by an active
18 file—for long periods of time before they are overwritten. In addition, a
19 computer's operating system may also keep a record of deleted data in a
20 "swap" or "recovery" file.
21
- 22 c. Wholly apart from user-generated files, computer storage media—in
23 particular, computers' internal hard drives—contain electronic evidence of
24 how a computer has been used, what it has been used for, and who has used
25 it. To give a few examples, this forensic evidence can take the form of
26 operating system configurations, artifacts from operating system or
27 application operation; file system data structures, and virtual memory
28 "swap" or paging files. Computer users typically do not erase or delete this
evidence, because special software is typically required for that task.
However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes
automatically downloaded into a temporary Internet directory or "cache."

20. *Forensic evidence.* As further described in Attachment B, this application
seeks permission to locate not only computer files that might serve as direct evidence of
the crimes described on the warrant, but also for forensic electronic evidence that
establishes how digital devices or other electronic storage media were used, the purpose
of their use, who used them, and when. There is probable cause to believe that this
forensic electronic evidence will be on any digital devices or other electronic storage

1 media located at the SUBJECT PREMISES, in the SUBJECT VEHICLE, and on SCOTT
2 ANTHONY ORTON because:

- 3 a. Stored data can provide evidence of a file that was once on the digital
4 device or other electronic storage media but has since been deleted or
5 edited, or of a deleted portion of a file (such as a paragraph that has been
6 deleted from a word processing file). Virtual memory paging systems can
7 leave traces of information on the digital device or other electronic storage
8 media that show what tasks and processes were recently active. Web
9 browsers, e-mail programs, and chat programs store configuration
10 information that can reveal information such as online nicknames and
11 passwords. Operating systems can record additional information, such as
12 the history of connections to other computers, the attachment of
13 peripherals, the attachment of USB flash storage devices or other external
14 storage media, and the times the digital device or other electronic storage
15 media was in use. Computer file systems can record information about the
16 dates files were created and the sequence in which they were created.
- 17 b. As explained herein, information stored within a computer and other
18 electronic storage media may provide crucial evidence of the “who, what,
19 why, when, where, and how” of the criminal conduct under investigation,
20 thus enabling the United States to establish and prove each element or
21 alternatively, to exclude the innocent from further suspicion. In my
22 training and experience, information stored within a computer or storage
23 media (e.g., registry information, communications, images and movies,
24 transactional information, records of session times and durations, internet
25 history, and anti-virus, spyware, and malware detection programs) can
26 indicate who has used or controlled the computer or storage media. This
27 “user attribution” evidence is analogous to the search for “indicia of
28 occupancy” while executing a search warrant at a residence. The existence
or absence of anti-virus, spyware, and malware detection programs may
indicate whether the computer was remotely accessed, thus inculcating or
exculpating the computer owner and/or others with direct physical access to
the computer. Further, computer and storage media activity can indicate
how and when the computer or storage media was accessed or used. For
example, as described herein, computers typically contain information that
log: computer user account session times and durations, computer activity
associated with user accounts, electronic storage media that connected with
the computer, and the IP addresses through which the computer accessed
networks and the internet. Such information allows investigators to
understand the chronological context of computer or electronic storage

media access, use, and events relating to the crime under investigation.² Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a digital device or other electronic storage media works can, after examining this forensic evidence in its proper context, draw conclusions about how the digital device or other electronic storage media were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device or other electronic storage media that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

² For example, if the examination of a computer shows that: (a) at 11:00am, someone using the computer used an internet browser to log into a bank account in the name of John Doe; (b) at 11:02am the internet browser was used to download child pornography; and (c) at 11:05 am the internet browser was used to log into a social media account in the name of John Doe, an investigator may reasonably draw an inference that John Doe downloaded child pornography.

- 1 e. Further, in finding evidence of how a digital device or other electronic
2 storage media was used, the purpose of its use, who used it, and when,
3 sometimes it is necessary to establish that a particular thing is not present.
4 For example, the presence or absence of counter-forensic programs or anti-
5 virus programs (and associated data) may be relevant to establishing the
6 user's intent.

7 **DIGITAL DEVICES AS INSTRUMENTALITIES OF THE CRIMES**

8 21. As set forth in detail above, there is probable cause to believe that SCOTT
9 ANTHONY ORTON transmitted the above-listed threats and solicitation for the murder
10 of Victim 1, in violation of 18 U.S.C. §§ 875(c) and 1958(a). The threats and
11 solicitations were transmitted via the Internet. Based on the facts set forth above, there is
12 probable cause to believe that SCOTT ANTHONY ORTON used a digital device to
13 connect to and transmit the messages via the Internet. The digital device(s) used to
14 transmit the messages are instrumentalities of 18 U.S.C. §§ 875(c) and 1958(a).

15 **PAST EFFORTS TO OBTAIN ELECTRONICALLY STORED INFORMATION**

16 22. Because of the type of the evidence sought and the nature of the
17 investigation, agents have not made any effort to obtain the evidence based on the
18 consent of SCOTT ANTHONY ORTON. I believe, based upon the nature of the
19 investigation and the information I have received, that if SCOTT ANTHONY ORTON
20 becomes aware that agents intend to search the SUBJECT PREMISES, SUBJECT
21 VEHICLE, and SCOTT ANTHONY ORTON in advance of the execution of a search
22 warrant, he may attempt to destroy evidence, thereby obstructing the investigation.

23 **REQUEST FOR AUTHORITY TO CONDUCT OFF-SITE SEARCH** 24 **OF TARGET COMPUTERS**

25 23. *Necessity of seizing or copying entire computers or storage media.* In most
26 cases, a thorough search of premises for information that might be stored on digital
27 devices or other electronic storage media often requires the seizure of the physical items
28 and later off-site review consistent with the warrant. In lieu of removing all of these
items from the premises, it is sometimes possible to make an image copy of the data on
the digital devices or other electronic storage media, onsite. Generally speaking, imaging

1 is the taking of a complete electronic picture of the device's data, including all hidden
 2 sectors and deleted files. Either seizure or imaging is often necessary to ensure the
 3 accuracy and completeness of data recorded on the item, and to prevent the loss of the
 4 data either from accidental or intentional destruction. This is true because of the
 5 following:

- 6 a. *The time required for an examination.* As noted above, not all evidence
 7 takes the form of documents and files that can be easily viewed on site.
 8 Analyzing evidence of how a computer has been used, what it has been
 9 used for, and who has used it requires considerable time, and taking that
 10 much time on premises could be unreasonable. As explained above,
 11 because the warrant calls for forensic electronic evidence, it is exceedingly
 12 likely that it will be necessary to thoroughly examine the respective digital
 13 device and/or electronic storage media to obtain evidence. Computer hard
 14 drives, digital devices and electronic storage media can store a large
 15 volume of information. Reviewing that information for things described in
 16 the warrant can take weeks or months, depending on the volume of data
 17 stored, and would be impractical and invasive to attempt on-site.
- 18 b. *Technical requirements.* Digital devices or other electronic storage media
 19 can be configured in several different ways, featuring a variety of different
 20 operating systems, application software, and configurations. Therefore,
 21 searching them sometimes requires tools or knowledge that might not be
 22 present on the search site. The vast array of computer hardware and
 23 software available makes it difficult to know before a search what tools or
 24 knowledge will be required to analyze the system and its data on the
 25 premises. However, taking the items off-site and reviewing them in a
 26 controlled environment will allow examination with the proper tools and
 27 knowledge.
- 28 c. *Variety of forms of electronic media.* Records sought under this warrant
 could be stored in a variety of electronic storage media formats and on a
 variety of digital devices that may require off-site reviewing with
 specialized forensic tools.

SEARCH TECHNIQUES

24. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal
 Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging,
 or otherwise copying digital devices or other electronic storage media that reasonably

1 appear capable of containing some or all of the data or items that fall within the scope of
2 Attachment B to this Affidavit, and will specifically authorize a later review of the media
3 or information consistent with the warrant.

4 25. Precision Home Inspection (the "Company"), a sole proprietorship owned
5 by SCOTT ANTHONY ORTON, is a functioning company that conducts legitimate
6 business. SCOTT ANTHONY ORTON operates the Company from the SUBJECT
7 PREMISES. The seizure of the Company's computers may limit the Company's ability
8 to conduct its legitimate business. As with any search warrant, I expect that this warrant
9 will be executed reasonably. Reasonable execution will likely involve conducting an
10 investigation on the scene of what computers, or storage media, must be seized or copied,
11 and what computers or storage media need not be seized or copied. Where appropriate,
12 officers will copy data, rather than physically seize computers, to reduce the extent of
13 disruption. If employees of the Company so request, the agents will, to the extent
14 practicable, attempt to provide the employees with copies of data that may be necessary
15 or important to the continuing function of the Company's legitimate business. If, after
16 inspecting the computers, it is determined that some or all of this equipment is no longer
17 necessary to retrieve and preserve the evidence, the government will return it.

18 26. Consistent with the above, I hereby request the Court's permission to seize
19 and/or obtain a forensic image of digital devices or other electronic storage media that
20 reasonably appear capable of containing data or items that fall within the scope of
21 Attachment B to this Affidavit, and to conduct off-site searches of the digital devices or
22 other electronic storage media and/or forensic images, using the following procedures:

23 **A. Processing the Search Sites and Securing the Data.**

24 a. Upon securing the physical search site, the search team will conduct an
25 initial review of any digital devices or other electronic storage media located at
26 the subject premises described in Attachment A that are capable of containing
27 data or items that fall within the scope of Attachment B to this Affidavit, to
28 determine if it is possible to secure the data contained on these devices onsite
in a reasonable amount of time and without jeopardizing the ability to
accurately preserve the data.

1
2 b. In order to examine the electronically stored information (“ESI”) in a
3 forensically sound manner, law enforcement personnel with appropriate
4 expertise will attempt to produce a complete forensic image, if possible and
5 appropriate, of any digital device or other electronic storage media that is
6 capable of containing data or items that fall within the scope of Attachment B
7 to this Affidavit.¹

8
9 c. A forensic image may be created of either a physical drive or a logical
10 drive. A physical drive is the actual physical hard drive that may be found in a
11 typical computer. When law enforcement creates a forensic image of a
12 physical drive, the image will contain every bit and byte on the physical drive.
13 A logical drive, also known as a partition, is a dedicated area on a physical
14 drive that may have a drive letter assigned (for example the c: and d: drives on
15 a computer that actually contains only one physical hard drive). Therefore,
16 creating an image of a logical drive does not include every bit and byte on the
17 physical drive. Law enforcement will only create an image of physical or
18 logical drives physically present on or within the subject device. Creating an
19 image of the devices located at the search locations described in Attachment A
20 will not result in access to any data physically located elsewhere. However,
21 digital devices or other electronic storage media at the search locations
22 described in Attachment A that have previously connected to devices at other
23 locations may contain data from those other locations.

24 d. If based on their training and experience, and the resources available to
25 them at the search site, the search team determines it is not practical to make an
26 on-site image within a reasonable amount of time and without jeopardizing the
27 ability to accurately preserve the data, then the digital devices or other
28 electronic storage media will be seized and transported to an appropriate law
enforcement laboratory to be forensically imaged and reviewed.

23 ¹ The purpose of using specially trained computer forensic examiners to conduct the
24 imaging of digital devices or other electronic storage media is to ensure the integrity of
25 the evidence and to follow proper, forensically sound, scientific procedures. When the
26 investigative agent is a trained computer forensic examiner, it is not always necessary to
27 separate these duties. Computer forensic examiners often work closely with investigative
28 personnel to assist investigators in their search for digital evidence. Computer forensic
examiners are needed because they generally have technological expertise that
investigative agents do not possess. Computer forensic examiners, however, often lack
the factual and investigative expertise that an investigative agent may possess on any
given case. Therefore, it is often important that computer forensic examiners and
investigative personnel work closely together.

1 **B. Searching the Forensic Images.**

2 a. Searching the forensic images for the items described in Attachment B may
 3 require a range of data analysis techniques. In some cases, it is possible for
 4 agents and analysts to conduct carefully targeted searches that can locate
 5 evidence without requiring a time-consuming manual search through unrelated
 6 materials that may be commingled with criminal evidence. In other cases,
 7 however, such techniques may not yield the evidence described in the warrant,
 8 and law enforcement may need to conduct more extensive searches to locate
 9 evidence that falls within the scope of the warrant. The search techniques that
 10 will be used will be only those methodologies, techniques and protocols as
 11 may reasonably be expected to find, identify, segregate and/or duplicate the
 12 items authorized to be seized pursuant to Attachment B to this affidavit. Those
 13 techniques, however, may necessarily expose many or all parts of a hard drive
 14 to human inspection in order to determine whether it contains evidence
 15 described by the warrant.

16 **REQUEST FOR SEALING**

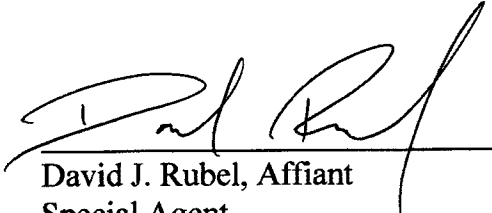
17 27. It is respectfully requested that this Court issue an order sealing, until
 18 further order of the Court, all papers submitted in support of this application, including
 19 the application, affidavit and search warrant. I believe that sealing this document is
 20 necessary because the items and information to be seized are relevant to an ongoing
 21 investigation and disclosure of the search warrant, this affidavit, and/or this application
 22 and the attachments thereto will jeopardize the progress of the investigation. Disclosure
 23 of these materials would give the target of the investigation an opportunity to destroy
 24 evidence, change patterns of behavior, notify confederates, or flee from prosecution.

25 **CONCLUSION**

26 28. Based on the foregoing, I believe there is probable cause that evidence,
 27 fruits, and instrumentalities of the violations of 18 U.S.C. § 875(c), which makes it crime
 28 to transmit in interstate or foreign commerce any communication containing any threat to
 kidnap any person or any threat to injure the person of another; and 18 U.S.C. § 1958(a),
 which makes it a crime to travel or cause another to travel in interstate or foreign
 commerce, or use or cause another to use the mail or any facility of interstate or foreign

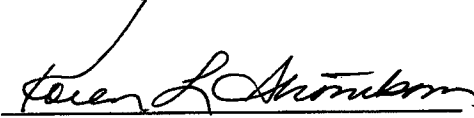
1 commerce, with intent that a murder be committed in violation of the laws of any State or
2 the United States as consideration for the receipt of, or as consideration for a promise or
3 agreement to pay, anything of pecuniary value, or conspire to do so are located at the
4 SUBJECT PREMISES, in the SUBJECT VEHICLE, and on SCOTT ANTHONY
5 ORTON as more fully described in Attachments A-1 through A-3 to this Affidavit, as
6 well as on and in any digital devices or other electronic storage media found at the
7 SUBJECT PREMISES, in the SUBJECT VEHICLE, and on SCOTT ANTHONY
8 ORTON. I therefore request that the court issue a warrant authorizing a search of the
9 SUBJECT PREMISES, SUBJECT VEHICLE and SCOTT ANTHONY ORTON as well
10 as any digital devices and electronic storage media located therein, for the items more
11 fully described in Attachment B hereto, incorporated herein by reference, and the seizure
12 of any such items found therein.

13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



David J. Rubel, Affiant
Special Agent
Federal Bureau of Investigation

SUBSCRIBED AND SWORN before me this 23rd day of November, 2015.



HON. KAREN L. STROMBOM
United States Magistrate Judge

ATTACHMENT A-1

The property to be searched is located at 5809 136th Street E, Puyallup, WA 98373, and includes any digital device(s) or other electronic storage media found therein. The property is further described as cream color one story house with yellow trim and an attached garage. The numbers 5809 are visible on the upper-right corner of the garage, facing the street.



ATTACHMENT A-2

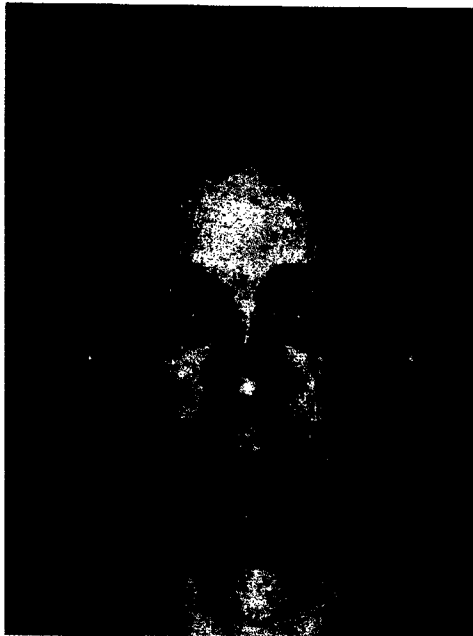
Vehicle to be searched: 2013 Dodge Ram with Washington license plate number B09802X, registered to SCOTT ANTHONY ORTON at 5809 136th Street E, Puyallup, WA 98373, and includes any digital device(s) or other electronic storage media found therein.

ATTACHMENT A-3

Person to be searched: SCOTT ANTHONY ORTON

SCOTT ANTHONY ORTON is a white male, approximately 6'0" with light brown hair and green eyes. His date of birth is [REDACTED] His photograph appears below.

The search of SCOTT ANTHONY ORTON shall include his person, clothing, and personal belongings, including backpacks, briefcases and bags, any digital device(s) and other electronic storage media found thereon/therein that are within his immediate vicinity and control at the location where the search warrant is executed within the Western District of Washington and that may contain the items called for by Attachment B to this warrant. It shall not include a body cavity or strip search.



ATTACHMENT B

I. ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. §§ 875(c) and 1958(a):

1. All records relating to violations of 18 U.S.C. §§ 875(c) and 1958(a) and involving SCOTT ANTHONY ORTON since September 18, 2012 including:

a. Any information recording SCOTT ANTHONY ORTON's schedule or travel itinerary from July 16, 2015, to the present;

b. Any weapons, including firearms;

c. Piano wire;

2. Any weapons, including firearms;

3. Piano wire;

4. Digital devices³ or other electronic storage media⁴ and/or their components, which include:

a. Any digital device or other electronic storage media capable of being used to commit, further, or store evidence of the offenses listed above;

³ "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

⁴ Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

1 b. Any digital devices or other electronic storage media used to
2 facilitate the transmission, creation, display, encoding or storage of data, including word
3 processing equipment, modems, docking stations, monitors, cameras, printers, plotters,
4 encryption devices, and optical scanners;

5 c. Any magnetic, electronic or optical storage device capable of storing
6 data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical
7 disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic
8 dialers, electronic notebooks, and personal digital assistants;

9 d. Any documentation, operating logs and reference manuals regarding
10 the operation of the digital device or other electronic storage media or software;

11 e. Any applications, utility programs, compilers, interpreters, and other
12 software used to facilitate direct or indirect communication with the computer hardware,
13 storage devices, or data to be searched;

14 f. Any physical keys, encryption devices, dongles and similar physical
15 items that are necessary to gain access to the computer equipment, storage devices or
16 data; and

17 g. Any passwords, password files, test keys, encryption codes or other
18 information necessary to access the computer equipment, storage devices or data.

19 4. Any digital devices or other electronic storage media that were or may have
20 been used as a means to commit the offenses described on the warrant, including to
21 transmit in interstate or foreign commerce any communication containing any threat to
22 kidnap any person or any threat to injure the person of another in violation of 18 U.S.C. §
23 875(c); to travel or cause another to travel in interstate or foreign commerce, or use or
24 cause another to use the mail or any facility of interstate or foreign commerce, with intent
25 that a murder be committed in violation of the laws of any State or the United States as
26 consideration for the receipt of, or as consideration for a promise or agreement to pay,
27 anything of pecuniary value, or conspire to do so, in violation of 18 U.S.C. § 1958(a).

28 5. For any digital device or other electronic storage media upon which
electronically stored information that is called for by this warrant may be contained, or
that may contain things otherwise called for by this warrant:

- a. evidence relating to the Fox Nation user accounts of Joseywhales and Joseywhales;
- b. evidence relating to [REDACTED] (also known as [REDACTED]);⁵
- c. evidence relating to StemExpress, LLC;
- d. evidence relating to reservations or plans to travel between July 16, 2015 and present;
- e. evidence of any communication with others regarding StemExpress, LLC, and/or [REDACTED];
- f. evidence relating to the identity and location of the SCOTT ANTHONY ORTON;
- g. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- h. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- i. evidence of the lack of such malicious software;
- j. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;
- k. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;
- l. evidence of the times the digital device or other electronic storage media was used;
- m. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

⁵ Referred to in the accompanying affidavit as Victim 1.

1 n. documentation and manuals that may be necessary to access the
2 digital device or other electronic storage media or to conduct a forensic examination of
3 the digital device or other electronic storage media;

4 o. contextual information necessary to understand the evidence
5 described in this attachment.

6 6. Records and things evidencing the use of Internet Protocol addresses
7 24.19.67.214 and 73.181.138.175 to communicate with nation.foxnews.com including:

8 a. routers, modems, and network equipment used to connect computers
9 to the Internet;

10 b. records of Internet Protocol addresses used;

11 c. records of Internet activity, including firewall logs, caches, browser
12 history and cookies, "bookmarked" or "favorite" web pages, search terms that the user
13 entered into any Internet search engine, and records of user-typed web addresses.

14 II. SEARCH PROTOCOL

15 In accordance with the information in the affidavit, law enforcement personnel
16 will execute the search of digital devices seized pursuant to this Attachment B as follows:

17 a. Upon securing the physical search site, the search team will conduct
18 an initial review of any digital devices or other electronic storage media located at the
19 subject premises described in Attachment A that are capable of containing data or items
20 that fall within the scope of this Attachment B, to determine if it is possible to secure the
21 data contained on these devices onsite in a reasonable amount of time and without
22 jeopardizing the ability to accurately preserve the data.

23 b. In order to examine the electronically stored information in a
24 forensically sound manner, law enforcement personnel with appropriate expertise will
25 attempt to produce a complete forensic image, if possible and appropriate, of any digital
26 device or other electronic storage media that is capable of containing data or items that
27 fall within the scope this of Attachment.

28 c. A forensic image may be created of either a physical drive or a
logical drive. A physical drive is the actual physical hard drive that may be found in a
typical computer. When law enforcement creates a forensic image of a physical drive,
the image will contain every bit and byte on the physical drive. A logical drive, also
known as a partition, is a dedicated area on a physical drive that may have a drive letter
assigned (for example the c: and d: drives on a computer that actually contains only one

1 physical hard drive). Therefore, creating an image of a logical drive does not include
2 every bit and byte on the physical drive. Law enforcement will only create an image of
3 physical or logical drives physically present on or within the subject device. Creating an
4 image of the devices located at the search locations described in Attachment A will not
5 result in access to any data physically located elsewhere. However, digital devices or
6 other electronic storage media at the search locations described in Attachment A that
7 have previously connected to devices at other locations may contain data from those
8 other locations.

9 d. If based on their training and experience, and the resources available
10 to them at the search site, the search team determines it is not practical to make an on-site
11 image within a reasonable amount of time and without jeopardizing the ability to
12 accurately preserve the data, then the digital devices or other electronic storage media
13 will be seized and transported to an appropriate law enforcement laboratory to be
14 forensically imaged and reviewed.

15 e. Searching the forensic images for the items described in this
16 Attachment B may require a range of data analysis techniques. The search techniques
17 that will be used will be only those methodologies, techniques and protocols as may
18 reasonably be expected to find, identify, segregate and/or duplicate the items authorized
19 to be seized pursuant to Attachment B to this affidavit.

20 f. If, after conducting its examination, law enforcement personnel
21 determine that any digital device is an instrumentality of the criminal offenses referenced
22 above, the government may retain that device during the pendency of the case as
23 necessary to, among other things, preserve the instrumentality evidence for trial, ensure
24 the chain of custody, and litigate the issue of forfeiture. If law enforcement personnel
25 determine that a device was not an instrumentality of the criminal offenses referenced
26 above, it shall be returned to the person/entity from whom it was seized within 90 days of
27 the issuance of the warrant, unless the government seeks and obtains authorization from
28 the court for its retention.

g. Precision Home Inspection (the "Company"), a sole proprietorship
owned by SCOTT ANTHONY ORTON, is a functioning company that conducts
legitimate business. SCOTT ANTHONY ORTON operates the Company from the
SUBJECT PREMISES. The seizure of the Company's computers may limit the
Company's ability to conduct its legitimate business. As with any search warrant, this
warrant will be executed reasonably. Reasonable execution will likely involve
conducting an investigation on the scene of what computers, or storage media, must be
seized or copied, and what computers or storage media need not be seized or copied.
Where appropriate, officers will copy data, rather than physically seize computers, to
reduce the extent of disruption. If employees of the Company so request, the agents will,

1 to the extent practicable, attempt to provide the employees with copies of data that may
2 be necessary or important to the continuing function of the Company's legitimate
3 business. If, after inspecting the computers, it is determined that some or all of this
4 equipment is no longer necessary to retrieve and preserve the evidence, the government
5 will return it.
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28